Assessoria de Tecnologia da Informação - ATI

Política de Segurança da Informação da Fundação João Pinheiro

Política Interna de Segurança da Informação da Fundação João Pinheiro

Política de Segurança da Informação da Fundação João Pinheiro

1. INTRODUÇÃO

O maior patrimônio de uma instituição está contemplado num tripé constituído por pessoas, processos e produtos (tecnologia), onde o valor agregado está intimamente ligado à qualidade desses elementos. A Fundação João Pinheiro - FJP possui como resultado dessa simbiose, vários estudos consolidados em documentos, imagens, gráficos, bases de dados estatísticos e demais acervos que ilustram o papel da instituição no cenário governamental.

Diante do enorme volume de informações estratégicas e necessárias às atividades da instituição, a FJP necessita de um arcabouço de medidas que suporte as mais variadas situações de segurança na qual os elementos do tripé estão envolvidos. A esse arcabouço denomina-se “Políticas de Segurança da Informação”. Este documento elenca algumas questões imprescindíveis para uma política eficiente e eficaz.

É fundamental que os gestores compreendam a importância da segurança da informação e todos os seus aspectos envolvidos, técnicas e informações que auxiliem a aprimorar a segurança do negócio da Fundação João Pinheiro.

Uma política de segurança da informação bem aplicada é capaz de mitigar ataques digitais, desastres tecnológicos ou falhas humanas, porém não blinda integralmente a instituição. Sempre existe a necessidade de aprimorar com finalidade de proteger as informações de brechas desconhecidas que podem causar enormes prejuízos para a instituição e que, muitas vezes são mais altas do que o custo para manter uma estrutura segura, íntegra, confiável e disponível. Como a segurança da informação se baseia nos quatro pilares: integridade, confidencialidade, disponibilidade e autenticidade, é necessário que as ações realizadas se dediquem a garantir esses pilares.

2. CONFIDENCIALIDADE E INFORMAÇÃO PESSOAL

Nos últimos anos, um aspecto que tem chamado muita atenção é a “Confidencialidade da Informação”. Principalmente quando se trata de informação pessoal. Como a Fundação João Pinheiro é uma instituição de pesquisa e ensino, deve-se ter a preocupação ao manipular dados sigilosos e pessoais adequando-se à LGPD (Lei Geral de Proteção de Dados Pessoais - Lei n° 13.709, de 14 agosto de 2018) no que tange à anonimização[1]dos dados. Abaixo alguns recortes da lei.

CAPÍTULO II
DO TRATAMENTO DE DADOS PESSOAIS

Seção I
Dos Requisitos para o Tratamento de Dados Pessoais

[1] Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

*IV - para a realização de estudos por **órgão de pesquisa**, garantida, sempre que possível, a **anonimização** dos dados pessoais;*

Seção II
Do Tratamento de Dados Pessoais Sensíveis

*Art. 13. Na realização de estudos em saúde pública, os **órgãos de pesquisa** poderão ter acesso a bases de dados pessoais, que serão tratados **exclusivamente dentro do órgão** e estritamente para a **finalidade de realização de estudos e pesquisas** e mantidos em **ambiente controlado e seguro**, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a **anonimização** ou **pseudonimização**[2] dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.*

*§ 1º A divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa de que trata o caput deste artigo em **nenhuma hipótese poderá revelar dados pessoais**.*

*§ 2º O órgão de pesquisa será o **responsável pela segurança da informação** prevista no caput deste artigo, não permitida, em circunstância alguma, a transferência dos dados a terceiro.*

Seção IV
Do Término do Tratamento de Dados

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

*II - estudo por **órgão de pesquisa**, garantida, sempre que possível, a **anonimização** dos dados pessoais;*

Para que essa adequação ocorra, é necessário que cada usuário tenha um perfil (conta) controlado que garanta que acesse somente os dados necessários para as tarefas da área que lhe compete. Cabendo ao gestor, o controle da administração desses dados evitando, por exemplo, o seu extravio ou mau uso. No caso da anonimização citada acima, deve-se ter a preocupação de suprimir qualquer informação que leve a identificação de uma pessoa.

3. INTEGRIDADE DAS INFORMAÇÕES E DISPONIBILIDADE DOS DADOS

Outra questão é a integridade das informações. Na FJP, deve-se ter um sistema de backup atualizado e fortemente robusto para ter a capacidade de armazenar e recuperar todo o acervo de informações da instituição. Nessa questão, é preciso enfatizar a priorização de armazenamento e recuperação dos dados mais relevantes e estratégicos. Essa medida visa restabelecer o funcionamento da FJP que pode ficar comprometido caso ocorra, por exemplo,

[2] Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

o corrompimento de sistemas de arquivo tanto em servidores como máquinas locais. Outros incidentes que podem ser atacados com essa medida são os tradicionais erros de disco rígido que normalmente corrompem os arquivos de dados.

Para manter a disponibilidade dos dados, a FJP deve dispor seu acervo em um ambiente que propicie aos usuários um acesso fácil e rápido por meio de uma interface amigável que demonstre a qualidade dos serviços da instituição e garanta a agilidade dos processos. Uma consideração muito importante a fazer é a implantação de um "**Sistema de Detecção de Intrusão – IDS**[3]" que monitore e bloqueie ataques de sequestro de dados ("ransomware[4]") e negação de serviços ("DDoS[5]") cujo objetivo é a indisponibilidade dos dados ou serviços. Adicionando à solução de IDS, tem-se também o Firewall[6] como barreira de proteção contra ataques de intrusão e negação de serviços. Importante salientar que não existe um sistema totalmente eficiente no combate a esses ataques, mas que diminuem a possibilidade de ocorrerem.

Como a FJP tem um Centro de Processamento de Dados próprio, é necessário o uso de equipamentos como "**Nobreak**" que propiciam a continuidade do funcionamento dos servidores assim como os demais ativos de rede, mesmo que ocorram quedas ou picos de energia elétrica.

Para garantir a segurança de dados, é fundamental garantir meios de autenticidade das informações preservadas. Como o acervo da FJP contempla vários documentos históricos e oficiais e tudo dentro de um ambiente governamental, faz-se necessário a garantia de que esses itens do acervo sejam autênticos evitando fraudes que possam causar graves problemas a longo prazo. Uma política de segurança que se enquadra nesse cenário é o uso de "**Assinaturas Digitais**" e "**Certificados Digitais**". Com essa garantia, o autor da informação não tem como recusar que ele é o verdadeiro autor. Esse subproduto da autenticidade é chamado de "**Não Repúdio**".

4. PRÁTICAS E AÇÕES

Diante das explanações postas neste documento, não basta apenas implementar as práticas de segurança da informação, é necessário minimizar as possíveis brechas e vulnerabilidades existentes. Para isso, se faz necessário aplicar ações elencadas, conforme descrito abaixo, dentre várias outras que se seguirão.

---

[3] IDS (*Intrusion detection System*) é um sistema de detecção de Intrusão na rede que geralmente trabalha no modo passivo. O seu modo *Inline* é conhecido como IPS (*Intrusion Prevention System*) que é capaz de fazer a detecção em tempo real. Em outras palavras o IDS é um sistema de configurações e regras que tem como objetivo gerar alertas quando detectar pacotes que possam fazer parte de um possível ataque.

[4] Ransomware é um tipo de software nocivo que restringe o acesso ao sistema infectado com uma espécie de bloqueio e cobra um resgate em criptomoedas para que o acesso possa ser restabelecido. Caso não ocorra o mesmo, arquivos podem ser perdidos e até mesmo publicados.

[5] Um ataque de negação de serviço é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus usuários. Alvos típicos são servidores web e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

[6] Em informática, um firewall é um dispositivo de uma rede de computadores, na forma de um programa ou de equipamento físico, que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP.

- **Acompanhar as tendências e evoluções da área de segurança da informação**, capacitando a equipe de TI com cursos, atualizando material de consulta sobre o assunto, pesquisando de forma contínua novas maneiras de se proteger quanto a ataques cibernéticos. Assim será possível implementar medidas de contenção modernas e rápidas no parque tecnológico da FJP;

- **Manter os softwares e drivers atualizados**. Um dos principais meios de acesso dos hackers aos sistemas é por meio de falhas encontradas em softwares (sistemas operacionais) e drivers. Elaborar ferramenta de controle com atualização de todos os softwares existentes na FJP passíveis de intrusão[7] e atualizá-la constantemente propagando-a para todo o parque tecnológico da instituição. As empresas fornecedoras desses softwares estão sempre lançando novas atualizações, corrigindo as falhas e tornando os sistemas mais seguros. A regularidade dessas ações diminuem as chances de invasão e consequentemente prejuízos financeiros e da imagem da FJP;

- **Estabelecer um controle de acesso para os colaboradores.** Com isso, evita-se um problema bem corriqueiro exemplificado por meio do acesso de um funcionário às informações não concernentes à sua área de atuação minimizando os riscos de, por exemplo, a exclusão de um arquivo muito importante e que, por sua vez, não estava presente em nenhum backup feito anteriormente. Evita-se também o vazamento de informações confidenciais ou estratégicas;

- **Estabelecer bloqueios de sistemas de saída.** Com esse mecanismo, evita-se que informações sejam vazadas sem o conhecimento da equipe da ATI. Assim é possível bloquear aplicativos e sites que facilitam o recolhimento de arquivos e envio para fora da rede da FJP. Fazem parte dessa ação, bloquear o uso de redes sociais e aplicativos de conversação que não favoreçam ao bom andamento dos trabalhos realizados na FJP;

- **Criar normas de conduta referente à utilização da tecnologia da informação na FJP.** Um dos objetivos dessa ação é evitar a entrada de "malwares" devido ao uso inadequado dessa tecnologia. Por exemplo, esse regramento inserido num programa de conscientização da política de segurança da informação da FJP, evita ou reduz a ação de um funcionário agir por conta própria, tentando solucionar um problema de sistema que deveria ser encaminhado para o setor competente. Criar ou evoluir uma cultura consciente do uso da tecnologia da informação de forma responsável e madura faz parte dessa ação. Esse tipo de documentação permite normatizar as regras utilizadas na FJP;

- **Treinar os colaboradores para medidas de segurança.** Políticas de segurança podem não ser tão claras para os colaboradores, principalmente por envolverem questões específicas da área de tecnologia da informação. O objetivo do treinamento é ensinar medidas básicas de segurança, normatizando as condutas de todos os envolvidos. Um exemplo de esclarecimento pelo treinamento é explicar as razões pelas quais, determinadas redes sociais são bloqueadas no ambiente organizacional. O treinamento ajuda também na uniformização de procedimentos em caso de problemas;

[7] Acessos não autorizados que podem indicar a ação de um cracker ou até mesmo de funcionários mal intencionados.

- **Ter ferramentas de monitoramento.** É imprescindível utilizar ferramentas de monitoramento de atividades no cotidiano da área de TI. Para que a segurança seja eficaz, é necessário saber o que está acontecendo em toda a rede diariamente. Qualquer tipo de conduta errada, vulnerabilidade, mudança nos padrões de acesso deve ser percebida imediatamente, de forma a ser contida e evitar um ataque digital;

- **Utilizar criptografia de dados.** Uma forma de contribuir de maneira segura para a circulação de informações estratégicas e confidenciais é a criptografia. Com isso, há o impedimento que arquivos sejam acessados indevidamente caso sejam interceptados no meio de uma transmissão;

- **Ter suporte de empresas especializadas em segurança da informação.** Como a equipe de TI da FJP possui poucos recursos na área de segurança da informação, é prudente ter uma consultoria por empresas especializadas no assunto para que oriente a respeito do emprego de novos mecanismos de proteção. Como essas empresas estão sempre pesquisando e desenvolvendo soluções inteligentes, essa ação ajuda a potencializar a segurança da informação na FJP. Um exemplo seria o armazenamento de backups na nuvem de forma segura, onde a infraestrutura é muito mais robusta e moderna tecnologicamente do que na FJP. Garante maior proteção para os dados e desafoga a equipe de TI para atender a outras demandas. Além disso, em caso de desastres, como o ransomware ("WannaCry[8]"), essas empresas especializadas poderão auxiliar na resolução da situação com a aplicação de protocolos para mitigar os danos causados pelo desastre.

- **Adotar a política da "Mesa Limpa".** Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não. Ao usar uma impressora coletiva, recolher o documento impresso imediatamente.

5. CENTRO DE PROCESSAMENTO DE DADOS - CPD

Como a Fundação João Pinheiro possui um CPD (Centro de Processamento de Dados) próprio, é necessário manter essa estrutura estratégica e valiosa, muito bem controlada e segura. Para isso, deve-se seguir algumas recomendações elencadas abaixo que são estritamente necessárias para zelar pelo bom funcionamento e principalmente a segurança dos ativos de rede e as informações armazenadas nos servidores do CPD da FJP.

- Possuir gerador de energia elétrica como "Nobreak" para manter os servidores em funcionamento temporariamente até o seu completo desligamento de forma normal, em caso de pane elétrica;
- Possuir um sistema de ar condicionado eficiente que mantenha a temperatura ideal do ambiente do CPD para o correto funcionamento dos equipamentos de TI;

[8] WannaCry é um crypto-ransomware que afeta o sistema operacional Microsoft Windows. A sua difusão em larga escala iniciou-se a 12 de maio de 2017 infectando mais de 230.000 sistemas.

- Separar as calhas por onde passam os fios elétricos e lógicos. Evitam-se com isso interferências;
- Controle de acesso ao ambiente CPD. Somente pessoas autorizadas devem permanecer nesse ambiente além da equipe de TI;
- Possuir um sistema de monitoramento por câmera que possa identificar qualquer pessoa que entra ou sai do ambiente;
- Possuir extintores próprios para o uso em equipamentos de TI, bem localizados, de fácil acesso e principalmente, dentro da validade;

6. OBRIGAÇÕES OPERACIONAIS

Para que uma "Política de Segurança da Informação" apresente bons resultados de acordo com o que se propõe acima, deve-se estabelecer obrigações operacionais como as descritas abaixo.

6.1 Utilização da Informação e Recursos

É de responsabilidade do Diretor/Gerente/Supervisor de cada unidade administrativa estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a descrição abaixo:

• Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.

• Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

• Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada desta informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

• Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada desta informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Diretor/Gerente deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

O acesso da informação deve ser autorizado apenas para os usuários que necessitam da mesma para o desempenho das suas atividades profissionais relacionadas à FJP. Esse conhecimento do usuário deve

ser utilizado apenas para o desenvolvimento e operacionalização do negócio da FJP.

Cada usuário deve acessar apenas informações e os ambientes previamente autorizados.

Qualquer tentativa de acesso a ambientes não autorizados será considerada uma violação desta política.

O acesso da informação armazenada e processada no ambiente de tecnologia é individual e intransferível. Esse acesso acontece por meio da identificação e autenticação do usuário.

Quando a autenticação for feita por meio do uso de senha, o usuário deve manter a mesma em segredo e não utilizar senhas óbvias, de forma que somente ele seja capaz de reproduzi-la.

Os documentos produzidos por intermédio dos sistemas de TI são de propriedade da FJP. De igual modo, os programas desenvolvidos para a FJP, por servidores do quadro ou prestadores de serviço.

São de propriedade da FJP todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a FJP.

As informações pertencentes à FJP ou instituição pública ou sob salvaguarda destes devem ser utilizadas apenas para os propósitos definidos na sua missão institucional.

Os recursos de tecnologia da organização, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.

6.2 Proteção e Continuidade no Uso da Informação

Toda informação deve ser protegida para que não seja alterada, acessada e destruída indevidamente. A informação armazenada em meio digital deve ser protegida contra desastre físico (fogo, água, calor, pane elétrica, etc.) e desastre lógico (vírus, alteração indevida da informação, etc.).

Toda informação crítica para o funcionamento da organização deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com proteção adequada.

Para criação das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e recuperação de ambiente.

Os recursos tecnológicos, de infraestrutura e os ambientes físicos devem ser protegidos contra desastres e contingências.

Os locais onde se encontram os recursos da organização devem ter proteção e controle de acesso físico compatível com seu nível de criticidade.

6.3 Dados dos Funcionários

A FJP se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários que

porventura sejam armazenados serão considerados dados confidenciais.

Dados Pessoais de Funcionários sob a responsabilidade da FJP não serão usados para fins diferentes daqueles para os quais foram coletados.

Os funcionários se comprometem a não armazenar dados pessoais nas instalações da instituição.

Mesmo que sejam armazenados dados pessoais a instituição não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados não devem ser armazenados nos diretórios dos servidores, e não devem fazer parte da rotina de backup da organização.

6.4 FJP - Funcionários, Temporários e Estagiários

A gerência de recursos humanos - GRH é a unidade responsável pelo Recrutamento e Seleção e Movimentação de Pessoal da Instituição e deverá:

Informar a ATI, sobre toda e qualquer movimentação de efetivos e/ou estagiários, e admissão/desligamento de funcionários, para que os mesmos possam ser cadastrados ou excluídos nos sistemas da Instituição. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pela ATI.

Cabe ao setor solicitante da contratação a comunicação a ATI sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço à Instituição, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso aos sistemas. No caso de desligamento, o setor de Recursos Humanos deverá comunicar o fato em tempo hábil à ATI, para que o funcionário desligado tenha seus acessos aos sistemas e dados bloqueados.

Cabe à unidade, via instrução normativa disponível na Intranet, dar conhecimento e obter as devidas assinaturas de concordância dos novos e dos atuais funcionários, estagiários, contratados e menores aprendiz contratados em relação à Política de Segurança da Informação da FJP. Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

6.5 Transferência de Servidores, Funcionários, Temporários e Estagiários.

Quando um efetivo for promovido ou transferido de seção ou gerência, a GRH deverá comunicar o fato a ATI, para que sejam feitas as adequações necessárias para o acesso do referido funcionário aos sistemas informatizados da Instituição.

6.6 Computação Pessoal e Móvel

Com relação aos equipamentos particulares como computadores, pendrives ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio da instituição e nem devem ser

conectados às redes da FJP com exceção de autorização expressa do responsável pelo setor e com a concordância da Assessoria de Tecnologia da Informação e Comunicação - ATI.

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro equipamento computacional, de propriedade da FJP, devem estar cientes de que:

• Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.

• A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

• É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

• O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre próximo;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.
- Em caso de furto:
    - Registre a ocorrência em uma delegacia de polícia;
    - Comunique ao seu superior imediato e a ATI;
    - Envie uma cópia da ocorrência para a direção superior ou chefia imediata.

6.7 Uso de Sistemas

O ambiente de tecnologia da informação da FJP só deve utilizar sistemas informatizados homologados pela ATI, quaisquer outros softwares e sistemas não podem ser instalados, copiados ou utilizados nesses ambientes. O uso de sistemas não homologados poderá pôr em risco a segurança da informação. Qualquer tentativa de instalação, cópia ou uso de sistemas não homologados pela FJP será considerada uma violação desta política.

É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na FJP.

Os softwares e dados não homologados, ou licenciados, podem ser previamente desinstalados ou apagados sem necessidade de aviso prévio.

Os sistemas homologados pela FJP devem registrar o uso e as ações de seus usuários internos e externos.

Os usuários não podem, em hipótese alguma, instalar qualquer tipo de "software" (programa) nos equipamentos da Instituição, cabendo essa responsabilidade a ATI.

Periodicamente, a ATI fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Os usuários que instalarem em seus computadores de trabalho tais programas não autorizados serão responsabilizados perante a Instituição por quaisquer problemas ou prejuízos causados oriundos desta ação, estando sujeitos às sanções previstas em lei.

6.8 Ambiente Real dos Sistemas

O ambiente do sistema computacional destinado à execução dos sistemas e dados reais (ambiente de produção) não deve ser utilizado para testes e outras atividades semelhantes.

A passagem de programas e dados para o ambiente de produção deve ser controlada e documentada de maneira a garantir a integridade e disponibilidade desse ambiente para realização do negócio.

6.9 Segurança e Integridade dos Dados

O gerenciamento do(s) banco(s) de dados no CPD é responsabilidade exclusiva da ATI, assim como a manutenção, alteração e atualização de equipamentos e programas.

6.10 Necessidade de novos Sistemas, Aplicativos e Equipamentos.

Na Política de Segurança da Informação da FJP a ATI é responsável pela definição de compra e substituição de Sistemas, Aplicativos e Equipamentos. Qualquer necessidade de novos Sistemas, Aplicativos ou Equipamentos de Informática devem ser planejados, até a etapa de especificações das futuras aquisições, com a ATI tendo o objetivo de não comprometer a integração com outros sistemas e ter requisitos mínimos de qualidade, ou permitir a aquisição de equipamentos que atendam especificações técnicas mínimas.

6.11 Correio Eletrônico

Outro aspecto muito importante no cenário da “Segurança da Informação” **é a utilização de e-mail de forma segura e responsável**. O uso do correio eletrônico da FJP é para fins corporativos e relacionados às atividades do colaborador dentro da instituição. Para isso, têm-se abaixo boas práticas que estão em conformidade com as diretivas informadas nos decretos e cartilhas governamentais.

- As mensagens de correio eletrônico sempre deverão **incluir assinatura** com o seguinte formato:
    - Nome do colaborador
    - Gerência ou departamento
    - Nome da instituição
    - Telefone(s)
    - Correio eletrônico
- Não responder a e-mails que solicitam recadastramento de senhas, dados de conta bancária, e de cartão de crédito, prêmios, promoções, sorteios, brindes, informações pessoais, informações confidenciais, documentos de identidade, CPF e outros que pareçam suspeitos;

- Não abrir e-mails de procedência desconhecida;
- Não abrir ou responder mensagens consideradas spam[9];
- Cuidados necessários com arquivos anexados ao e-mail (principalmente com extensão .exe, .scr, .com, .bat, .doc, .dot, .xls, .mdb entre outras) que podem ser malwares (programas mal intencionados). A mensagem também pode conter redirecionamento para sites não confiáveis;
- Efetivar verificação criteriosa sobre a empresa ou pessoa que esteja solicitando informações e na dúvida, não responder ao solicitado. Em caso de suspeita, deve-se apagar imediatamente a mensagem do computador;
- Antes de abrir qualquer arquivo anexo, mesmo que de origem conhecida, verificar com um programa antivírus que deve estar sempre ativo e atualizado;
- Não abrir arquivos anexos ao e-mail cujo título informe sobre fotos de uma celebridade, morte ou acidente de um artista, calamidades, etc. Estes assuntos bombásticos são alvos de golpistas e fraudadores;
- Não responder e-mails de bancos ou instituições financeiras. Essas empresas não se comunicam por meio de e-mails, pois possuem canais de relacionamento que são divulgados aos clientes. Se gerar dúvidas sobre a legitimidade de uma mensagem, entrar em contato com a pessoa ou instituição para ter certeza de que não se trata de uma fraude;
- Se não for interessante receber propagandas não divulgar seu e-mail em lojas ou qualquer estabelecimento comercial físico ou virtual;
- Em sites institucionais, evite expor diretamente os e-mails, existem robôs especializados na extração de e-mails. Utilizar formulários de contato ou então imagens, para dificultar a ação desses robôs;
- Evitar expor o e-mail em redes sociais;
- As chaves para um bom e-mail são clareza, concisão e precisão;
- Não é recomendável enviar e-mails para muitos usuários. Isso pode ser detectado por outros programas de e-mail como “spam”. Utilize o menor número de destinatários possível, geralmente em torno de 25. Sempre que precisar enviar para vários destinatários, faça uso de listas de distribuição;
- Fazer uso do compartilhamento de arquivos, portanto evitar encaminhar anexos de grande tamanho;

As mensagens de correio eletrônico são instrumentos de comunicação interna e externa para realização de negócio da FJP. Elas devem ser escritas em linguagem profissional e que não comprometa a imagem da FJP, não vá de encontro à legislação vigente e nem aos princípios éticos da FJP. Mensagens fora dessas características não devem ser enviadas.

O conteúdo do correio eletrônico de cada usuário pode ser acessado pela FJP quando de situações que ponham em risco a sua imagem e o seu negócio. Este acesso será feito a critério da FJP, mediante comunicação ao superior imediato do usuário e à ATI, e deve ser registrado formalmente permitindo uma auditoria desse procedimento.

9

O termo Spam é um acrônimo derivado da expressão em inglês "Sending and Posting Advertisement in Mass", traduzido em português "Enviar e Postar Publicidade em Massa".

É terminantemente proibido o envio de mensagens que:

• Contenham declarações difamatórias e linguagem ofensiva;

• Possam trazer prejuízos a outras pessoas;

• Sejam hostis e desnecessárias;

• Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

• Possam prejudicar a imagem da organização;

• Possam prejudicar a imagem de outras empresas;

• Sejam incoerentes com as políticas da FJP.

6.12 Uso da Internet

O ambiente de Internet deve ser usado para o desempenho das atividades profissionais do usuário para a FJP. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados. O uso da Internet será monitorado pela ATI, inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da FJP, sem expressa anuência da ATI, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites, exceto mediante solicitação de exceção aprovada pela ATI:

• De estações de rádio, TV, jogos, filmes, mesmo através de dispositivos USB;

• De conteúdo pornográfico ou correlato;

• Que defendam atividades ilegais;

• Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

• Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da FJP;

• Que promovam discussão pública sobre os negócios da FJP, a menos que autorizado pela Diretoria;

• Que possibilitem a distribuição de informações de nível “Confidencial”.

• Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

6.13 Permissões e Senhas

Um ponto muito importante e que requer muita atenção é quanto à **autenticação e senha**. O colaborador é responsável por todos os atos executados com seu identificador (login), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso às informações e aos recursos de tecnologia. Os colaboradores devem:

- Manter a confidencialidade, memorizar e não registrar a senha em lugar algum;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento da mesma;
- Criar senhas de qualidade, que sejam de difícil adivinhação;
- Impedir o uso do seu equipamento por outras pessoas enquanto este estiver “logado” com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar (Ctrl + Alt + Del).

Todo usuário para acessar sistemas corporativos da FJP deve possuir um login e senha previamente cadastrados por funcionários da ATI.

A chefia imediata do funcionário deve preencher uma ficha com informações de quais sistemas e dados o novo usuário terá direito de acesso, e quais serão restritos, e encaminhar a ATI.

As senhas devem ter período de validade de no máximo 90 dias, e apresentem um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc.) devem comunicar a ATI qual será o seu substituto quando de sua ausência da FJP, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pela ATI.

6.14 Uso de Antivírus

Todo arquivo em mídia proveniente de entidade externa a FJP deve ser verificado por programa antivírus.

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

6.15 Compartilhamento de Dados

Todos os dados deverão ser armazenados nos servidores de rede, e a autorização para acessá-los deverá ser fornecida pelo Servidor AD (Active Directory[10]).

Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso do AD. É monitorado na instituição o compartilhamento de dispositivos móveis tais como pendrives e outros.

[10] O Active Directory é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambiente Windows.

6.16 Backup (Cópia de Segurança dos Dados)

Todos os dados de sistemas corporativos da FJP devem ser protegidos através de rotinas automatizadas de backup, todos os dados contidos nas pastas de rede da FJP possuem esta rotina automatizada.

6.17 Cópias de Segurança de Arquivos em Desktop

Não é política da FJP o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais, por exemplo, que não permitem o armazenamento em rede.

Nestes e em outros casos, os funcionários devem comunicar a ATI para que façam backup dos dados de suas respectivas máquina periodicamente. É responsabilidade dos usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho que estejam fora das pastas de rede.

6.18 Documentação

Todos os procedimentos que possibilitem a proteção da informação e continuidade do seu uso devem ser documentados, de tal forma que possibilite que a organização continue a operacionalização desses procedimentos, mesmo na ausência do usuário responsável.

Os bens de informação da FJP devem ser inventariados e classificados quanto à criticidade de acesso a esses recursos.

7. “SEGURANÇA DA INFORMAÇÃO” NO AMBIENTE DE TELETRABALHO

- Utilizar documentos compartilhados em nuvem (“Storage Cloud”) com senha e ter sempre revisor para gerenciar o uso e conteúdo das informações. Sempre que possível, evitar compartilhamento aberto a todos, principalmente quando forem informações estratégicas à FJP;
- Possuir mecanismo de auditoria nos documentos que identifique a pessoa que está manipulando o documento compartilhado ao editar, copiar, excluir, imprimir, etc.;
- Usar ferramentas de colaboração e videoconferência de forma consciente. Disponibilizar reunião, orientando os convidados a fechar câmeras e microfone e utilizar esses recursos somente quando estritamente necessário. Com isso evitam-se interferências e minimiza o uso da banda de internet. Nesse aspecto, a política trata do pilar disponibilidade da informação;
- Com o advento do “teletrabalho” têm-se a falsa sensação de segurança no ambiente. Na verdade existem menos barreiras de segurança a ultrapassar. Diante desse novo cenário, ter um software antivírus atualizado que acompanha rotineiramente o surgimento de novas ameaças é recomendação da política de segurança da informação;

- Conscientizar os colaboradores sobre ataques oriundos do correio eletrônico. A maior parte dos ataques advêm de cliques consentidos e não de procedimentos involuntários;
- Com o aumento da carga e uso de serviços eletrônicos utilizados remotamente, deve-se monitorá-los para garantir um perfeito funcionamento;
- Evitar trabalhar em ambientes públicos ou em redes Wi-Fi públicas para acessos à dados institucionais;
- Utilizar backup na “nuvem” com finalidade de restaurar os dados independentemente de localização e automatizar as rotinas de cópias de arquivos. Recomenda-se utilização da ferramenta institucional, o “Google Drive”.

8. LEGISLAÇÕES E REGULAMENTAÇÕES

- Decreto Estadual n° 46.226, de 24/04/2013: Dispõe sobre o uso de correio eletrônico institucional no âmbito da Administração Pública Direta, Autárquica e Fundacional do Poder Executivo.

Acesso disponível em:

https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=DEC&num=46226&comp=&ano=2013

- Decreto Estadual n° 44.998, de 30/12/2018: Institui a Política de Tecnologia da Informação e Comunicação no Governo do Estado de Minas Gerais, cria o Sistema de Governança de Tecnologia da Informação e Comunicação e o Comitê Executivo de Tecnologia da Informação e Comunicação no âmbito da Administração Pública Estadual.

Acesso disponível em:

https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=DEC&num=44998&comp=&ano=2008

- Resolução Seplag 107 de 26-12-2018: Regulamenta a política da segurança da informação no que se refere à utilização da Tecnologia da Informação e Comunicação pelos usuários dos Órgãos e Entidades do Poder Executivo da Administração Pública Estadual Direta, Autárquica e Fundacional.

Acesso disponível em:

http://planejamento.mg.gov.br/sites/default/files/documentos/gestao-governamental/gestao-de-ti/resolucao_seplag_107_2018_-_seguranca.pdf

- Resolução Conjunta SEPLAG/CGE/SEF/AGE/PRODEMGE n° 10.064/2019: Institui o Grupo de Trabalho sobre a Lei Geral de Proteção de Dados no âmbito do Governo do Estado de Minas Gerais.

Acesso disponível em:

http://planejamento.mg.gov.br/sites/default/files/documentos/gestao-governamental/gestao-de-ti/1_-_resolucao_conjunta_seplag_cge_sef_age_prodemge_10064_2019.pdf

- Decreto Estadual n° 45.241, de 10/12/2009: Dispõe sobre o acesso às novas ferramentas interativas da Web 2.0 em uso nos órgãos e entidades da Administração Pública Estadual.

Acesso disponível em:

https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=DEC&num=45241&comp=&ano=2009

- Decreto Estadual n° 45.969, de 24/05/2012: Regulamenta o acesso à informação no âmbito do Poder Executivo.

Acesso disponível em:

https://www.almg.gov.br/consulte/legislacao/completa/completa.html?tipo=DEC&num=45969&comp=&ano=2012

Referências bibliográficas:

AC ONLINE Brasil. Política de Segurança da Autoridade Certificadora ONLINE BRASIL. Disponível em:

http://icp-brasil.validcertificadora.com.br/ac-onlinebrasil/ps-ac-onlinebrasil.pdf. Acesso em: Junho/2020.

ECOIT. Segurança da informação: o que é e 12 dicas práticas para garantir. Disponível em: https://ecoit.com.br/seguranca-da-informacao/. Acesso em: Junho/2020.

Governo Federal, Secretaria-Geral. Disponível em: http://legislacao.planalto.gov.br/legisla/legislacao.nsf/Viw_Identificacao/lei%2013.709-2018?OpenDocument. Acesso em: Junho/2020.

ITeam. Política de Segurança da Informação (PSI). Disponível em: https://it-eam.com/psi2018.pdf. Acesso em: Junho/2020.

International Organization Standardization – ISO. Norma ISO/IEC 27000, Information security management systems. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip. Acesso em: Junho/2020.

SENAC/SP. Política de Segurança da Informação (PSI). Disponível em: http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf. Acesso em: Junho/2020.

UFRJ. Sistemas de detecção de intrusão (IDS). Disponível em: https://www.gta.ufrj.br/grad/16_2/2016IDS/conceituacao.html. Acesso em: Junho/2020.

USP. Cartilha de boas práticas para o uso de e-mails e segurança da informação. Disponível em: https://www.sti.usp.br/cartilha-de-boas-praticas-para-o-uso-de-emails-e-seguranca-da-informacao/. Acesso em: Junho/2020.

ITCHANNEL. Sim ao Teletrabalho, mas não de qualquer forma. Disponível em: www.itchannel.pt/news/seguranca/sim-ao-teletrabalho-mas-nao-de-qualquer-forma. Acesso em: Agosto/2020.

BHS. 7 passos para implementar uma política de trabalho remoto. Disponível em: www.bhs.com.br/2020/04/22/7-passos-para-implementar-uma-politica-de-trabalho-remoto. Acesso em: Agosto/2020.

FACEBOOK. Contas invadidas por hackers. Disponível em: http://facebook.com/help/instagram. Acesso em: Agosto/2020.